

REMARKS

Claims 1-66 are currently pending in the subject application, and are presently under consideration. Claims 1-66 are rejected. Favorable reconsideration of the application is requested in view of the amendments and comments herein.

I. Rejection of Claims 11-14, 16-22, 24-28, 42-45, 47-51-53, 55, 57-59, and 63-66 Under 35 U.S.C. §102(e)

Claims 11-14, 16-22, 24-28, 42-45, 47-51-53, 55, 57-59, and 63-66 stand rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,301,658 to Koehler ("Koehler"). Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claims 11 and 42 recite a method and computer program, respectively, of replacing an expiring role certificate comprising displaying a list of roles to a user who is either a role member or a role administrator, wherein the user is a member of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members. Claims 11 and 42 recite elements that are to be performed to/for a role certificate, such that the role certificate can be utilized by a user that is a member of a group as a group stamp and for encryption of information which may be decrypted by a plurality of group members. As described in the response to the Office Action dated November 10, 2004, the digital certificates taught by Koehler are user digital certificates (see Kohler, *e.g.*, col. 3, line 46; col. 3, line 62; and col. 4, line 8), which are "conventional" digital certificates (see Kohler, *e.g.*, col. 4, line 46 and col. 4, line 57 through col. 5, line 41) in the discussion of the problems solved by Koehler. The Office Action dated May 3, 2005, asserts that Koehler teaches a "role certificate used by a group whereby they can encrypt and decrypt information." (Office Action dated May 3, 2005, page 3, citing Koehler, col. 3, ll. 1-11). Representative for Applicant respectfully disagrees with this assertion.

Koehler at no point discusses the use of a role certificate that can be utilized as a member of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members, as recited in claim 11.

The cited section of Koehler describes that authentication hierarchies provide a highly secure environment, accommodate diverse security groups, and allow the issuance and maintenance of certificates to be distributed across the organization (Koehler, col. 3, ll. 1-4). This cited section teaches nothing about a role certificate that can be used as a group stamp and for encryption of information which may be decrypted by a plurality of group members, as recited in claims 11 and 42. The Office Action dated May 3, 2005, further asserts that Koehler teaches that a role certificate is used “for encryption of information and decryption (authenticated) by group members.” (Office Action dated May 3, 2005, page 4, citing Koehler, col. 4, ll. 23-32). The cited section of Koehler teaches “a cache having entries for previously authenticated digital certificates issued by a certification authority (CA)” and that “a digital signature of the digital certificate of one of the CA’s is authenticated when a timestamp of the corresponding cache entry is older than a timestamp of the cache entry for the digital certificate of the corresponding parent CA.” (Koehler, col. 4, ll. 23-32). This cited section also teaches nothing about a role certificate that can be used for encryption of information which may be decrypted by a plurality of group members, as recited in claims 11 and 42. Encryption and decryption of a digital certificate is a separate and distinct issue from the authentication of a digital signature certificate. Furthermore, the cited section teaches that it is a certification authority’s certificate that is authenticated, and not the role certificate of a role member or role administrator, as defined by claims 11 and 42. Accordingly, Koehler does not contemplate a role certificate that can be used by a user who is either a role member or a role administrator, such that the user is a member of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members, as recited in claims 11 and 42.

In addition, claims 11 and 42 further recite selecting a role which is about to expire for renewal by the user, determining if the user is authorized to renew the role based upon verification of the user’s personal digital signature, generating a new role certificate having a private and public key, and transmitting the new role certificate to the user. An argument was proffered in the response to the Office Action dated November 10, 2004, that these elements of claims 11 and 42 are not taught by Koehler (Response to Office Action dated November 10,

2004, pages 21-22). However, the Office Action dated May 3, 2005, does not address these arguments in the Response to Arguments section beginning on page 2, and instead maintains the same rejection with the same citations of Koehler. Representative for Applicant therefore reiterates the previously stated arguments below and respectfully requests that the Examiner consider them.

The Office Action dated May 3, 2005, asserts that the above cited elements of claims 11 and 42 are taught by Koehler by stating that “Koehler discloses the role certificate where a role is selected from a list which is about to expire and replacing it with a new certificate having private and public keys.” (Office Action dated May 3, 2005, page 4, citing Koehler, col. 3, ll. 11-33). Koehler teaches that a certificate revocation list can be maintained that lists revoked and expired certificates, prompting authentication of a certificate against the revocation list (Koehler, col. 3, ll. 12-19), and further teaches that systems may cache expiration periods for certificates, such that expired certificates are removed and new certificates are authenticated (Koehler, col. 3, ll. 25-30). However, neither of these cited sections, nor any other sections of Koehler, teach selecting a role which is about to expire for renewal by the user, determining if the user is authorized to renew the role based upon verification of the user's personal digital signature, generating a new role certificate having a private and public key, and transmitting the new role certificate to the user, as recited in claims 11 and 42.

Accordingly, for the reasons stated above, Koehler does not anticipate claims 11 and 42. Withdrawal of the rejection of claim 11, as well as claims 12-16 which depend therefrom, and claim 42, as well as claims 43-47 which depend therefrom, is respectfully requested.

Claims 12 and 42 recite transmitting a new role certificate to the user over an encrypted secure communications line. Claims 12 and 43 depend from claims 11 and 42, respectively, and should be allowable for at least the reasons described above with regard to claims 11 and 42. In addition, the Office Action dated May 3, 2005, asserts that claim 12 is taught by Koehler (Office Action dated May 3, 2005, page 4, citing Koehler, col. 2, ll. 39-50 and 7-15). Representative for Applicant respectfully disagrees. Koehler teaches encryption of a transmission using a sender's private key that is decrypted using the sender's public key, allowing a receiver to trust that the

communication came from the claimed sender (Koehler, col. 2, ll. 7-15). Koehler further teaches that a sender of a message attaches a digital certificate to the message, the authenticity of which is verified by a recipient by verifying the digital signature of a certification authority that is encapsulated in the message, and then by verifying the sender's digital signature (Koehler, col. 2, ll. 39-50). Neither of these cited sections teach that a new role certificate is transmitted over a secure communications line, as recited in claims 12 and 43. The cited sections merely teach that a message is encrypted by a sender and decrypted by a recipient for authentication of the sender. Therefore, Koehler does not anticipate claims 12 and 43. Withdrawal of the rejection of claims 12 and 43 is respectfully requested.

Claims 16, 21, 24, 28, 52, 55, and 59 recite that the role certificate comprises a public key, a private key, a signature algorithm ID, a validity period, extensions, and at least one policy. Claim 16 depends from claim 11, claim 21 depends from claim 17, claim 24 depends from claim 22, claim 28 depends from claim 26, claim 52 depends from claim 48, claim 55 depends from claim 53, and claim 59 depends from claim 57. Therefore, claims 16, 21, 24, 28, 52, 55, and 59 should be allowable for the same reasons as described above and below regarding claims 11, 17, 22, 26, 48, 53, and 57, respectively. Additionally, the Office Action dated May 3, 2005, asserts that Koehler teaches claims 16, 21, 24, 28, 52, 55, and 59 by stating in the Response to Arguments that Koehler teaches extensions and at least one policy by issuer and user privileges (Office Action dated May 3, 2005, citing Koehler, col. 6, ll. 5-8). Representative for Applicant respectfully disagrees. Koehler teaches that a verification server maintains a verification cache that is a cache entry for each authenticated digital certificate (Koehler, col. 5, ll. 64-67), and that the verification cache is organized for efficient lookup of an item and is organized by owner and information type, with each cache entry storing information such as the item's timestamp, expiration data, issuer and user privileges (Koehler, col. 6, ll. 3-8). Koehler thus teaches that the issuer and user privileges are contained within the verification cache that is located on a verification server, and not within a digital certificate. Therefore, Koehler does not teach that a certificate (role certificate or otherwise) comprises extensions and at least one policy, as recited in claims 16, 21, 24, 28, 52, 55, and 59. Accordingly, Koehler does not anticipate claims 16, 21,

24, 28, 52, 55, and 59. Withdrawal of the rejection of claims 16, 21, 24, 28, 52, 55, and 59 is respectfully requested.

Claims 17 and 48 recite a method and computer program, respectively, of revoking a role certificate used as an organizational stamp and for organizational encryption by authorized members of the organization comprising transmitting a signature certificate to a registration web server by a user, wherein the user is a member of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members. As described above with regard to claims 11 and 42, Koehler does not teach the use of a role certificate, and thus claims 17 and 48 should be allowable.

In addition, claims 17 and 48 further recite transmitting a signature certificate to a registration web server by a user, authenticating by accessing a directory that the user is still a member of the organization, listing roles of which the user is a role member or a role authority, and removing the role certificate associated with the role from a directory database. The Office Action dated May 3, 2005, (at page 5) cites the same sections of Koehler as those cited for the rejection of claims 11 and 42 to assert that claims 17 and 48 are taught by Koehler (particularly, col. 3, ll. 12-19 and col. 3, ll. 25-30). However, claims 11 and 17 (as well as claims 42 and 48) each claim methods for achieving different results, such that the Office Action dated May 3, 2005, is interpreting the teachings of Koehler in two separate and conflicting ways. It is respectfully submitted that this argument was proffered in the response to the Office Action dated November 10, 2004 (Response to Office Action dated November 10, 2004, page 24), but was not addressed in the Response to Arguments section of the Office Action dated May 3, 2005. Representative for Applicant therefore reiterates the previously stated argument below and respectfully requests that the Examiner consider it.

The Office Action dated May 3, 2005, cites Koehler to teach “registration and certification.” (Office Action dated May 3, 2005, page 3, citing Koehler, col. 2, ll. 51-55). This counterargument and associated citation is extremely deficient in its attempt to provide an adequate rejection of claims 17 and 48. Claims 17 and 48 do not recite “certification” as described in the Response to Argument citation; the word “certification” is completely absent

altogether from claims 17 and 48. The cited section of Koehler in the Response to Arguments of the Office Action dated May 3, 2005, teaches an advantage of using digital certificates in that an authentication hierarchy corresponding to an organization's hierarchical structure can be established, thus facilitating public key registration and certification (Koehler, col. 2, ll. 51-55). This cited section is unrelated to the recitations of claims 17 and 48 in that it teaches nothing about a registration web server, authentication of whether a user is still a member of an organization, roles associated with a role member, and removing a role certificate associated with a role. Koehler does not teach, neither in the cited section nor anywhere else, transmitting a signature certificate to a registration web server by a user, authenticating by accessing a directory that the user is still a member of the organization, listing roles of which the user is a role member or a role authority, and removing the role certificate associated with the role from a directory database, as recited in claims 17 and 48. Accordingly, Koehler does not anticipate claims 17 and 48. Withdrawal of the rejection of claim 17, as well as claims 18-21 which depend therefrom, and claim 48, as well as claims 49-52 which depend therefrom, is respectfully requested.

Claims 18 and 49 recite that when the role certificate is removed from the directory database, the role associated with the role certificate remains intact on the database. Claims 18 and 49 depend from claims 17 and 48, respectively, and should thus be allowable for at least the reasons described above with regard to claims 17 and 48. The Office Action dated May 3, 2005, asserts that Koehler teaches claims 18 and 49 by stating, in the Response to Arguments, that "Koehler discloses the removal of certificate." (Office Action dated May 3, 2005, page 3, citing Koehler, col. 3, ll. 11-33). This statement is correct; Koehler teaches that, when an expired item is replaced by the issuing authority, the systems remove the old item (col. 3, ll. 27-29). However, this statement does not adequately support the rejection of claims 18 and 49. Specifically, as argued in the response to the Office Action dated November 10, 2004, Representative for Applicant argued that Koehler fails to teach that *the role associated with the role certificate remains intact on the database* when the role certificate is removed from the directory database, as recited in claims 18 and 49 (Response to Office Action dated November 10, 2004, page 25, emphasis added). The Office Action dated May 3, 2005, does not address the

above emphasized language in the rejection of claims 18 and 49. Additionally, because Koehler teaches that expired items are replaced and removed by the systems, Koehler teaches away from that which is recited in claims 18 and 49 in that claims 18 and 49 recite that the role associated with the role certificate remains intact on the database. Therefore, Koehler does not anticipate claims 18 and 49. Withdrawal of the rejection of claims 18 and 49 is respectfully requested.

Claims 19 and 50 recite establishing a secure encrypted communications line with the user and transmitting the role certificate to the user. Claims 19 and 50 depend from claims 17 and 48, and should thus be allowable for at least the reasons described above with regard to claims 17 and 48. Additionally, as described above regarding claims 12 and 43, Koehler does not teach a secure encrypted communications line over which a role certificate is transmitted to a user, as recited in claims 19 and 50. Accordingly, Koehler does not anticipate claims 19 and 50. Withdrawal of the rejection of claims 19 and 50 is respectfully requested.

Claims 22 and 53 recite a method and computer program, respectively, of recovery of an expired role certificate associated with the role used for organizational encryption and as an organizational stamp...wherein a role member is an entity having a right to digitally sign organizational documents using the role certificate and decrypting information sent to members of the organization which has been encrypted using the role certificate. As described above with regard to claims 11 and 42, Koehler does not teach the use of a role certificate, and thus claims 22 and 53 should be allowable.

In addition, the Office Action dated May 3, 2005, asserts that "Koehler discloses the recovery of an expired certificate via a timestamp cache which updates the old item." (Office Action dated May 3, 2005, page 6, citing Koehler, col. 4, ll. 17-40). Representative for Applicant respectfully disagrees with this assertion, as the cited section of Koehler is inapplicable to claims 22 and 53, and further inapplicable to what is asserted by the Office Action. The cited section of Koehler teaches that authentication of a user digital certificate is a function of a timestamp of both the user digital certificate and a chain of certifying authorities, and that timestamps for authenticated digital certificates in a cache entry are updated when the

digital signature is authenticated (Koehler, col. 4, ll. 17-40). This cited section of Koehler teaches nothing about recovery of expired role certificates, as recited in claims 22 and 53.

The Office Action dated May 3, 2005, further asserts that Koehler discloses “transmitting a request to recover expired certificates digitally signing with role certificate and decrypting.” (Office Action dated May 3, 2005, page 6, citing Koehler, col. 2, ll. 5-15). Representative for Applicant respectfully disagrees with this assertion, as the cited section of Koehler is also inapplicable to claims 22 and 53, and further inapplicable to what is asserted by the Office Action. As described above regarding claims 12 and 43, this cited section teaches encryption of a transmission using a sender’s private key that is decrypted using the sender’s public key, allowing a receiver to trust that the communication came from the claimed sender (Koehler, col. 2, ll. 7-15). This cited section teaches nothing about transmitting a request to recover an expired role certificate along with a digital signature from a role member, as recited in claims 22 and 53.

The Office Action dated May 3, 2005, further asserts that Koehler discloses “that a list contains role members.” (Office Action dated May 3, 2005, page 6, citing Koehler, col. 3, ll. 11-13). Representative for Applicant respectfully disagrees with this assertion, as the cited section of Koehler is also inapplicable to claims 22 and 53, and further inapplicable to what is asserted by the Office Action. This cited section teaches a certificate revocation list listing certificates which have been revoked and are no longer to be trusted (Koehler, col. 3, ll. 11-13). This cited section teaches nothing about listing all roles that the role member is listed as a role member on, as recited in claims 22 and 53.

The Office Action dated May 3, 2005, further asserts that Koehler discloses “contacting authority for copy of the role certificate...and transmitting the certificate” (Office Action dated May 3, 2005, page 6, citing Koehler, col. 4, ll. 7-12, and col. 2, ll. 23-25, respectively). Representative for Applicant respectfully disagrees with this assertion, as the cited section of Koehler is also inapplicable to claims 22 and 53, and further inapplicable to what is asserted by the Office Action. The first cited section teaches authenticating a user digital certificate issued by a certification authority that belongs to a hierarchy of certification authorities, with each certifying authority having a corresponding digital certificate (Koehler, col. 4, ll. 7-12). This

cited section teaches nothing about contacting a key authority for a copy of the role certificate, as recited in claims 22 and 53. Furthermore, the second cited section teaches transmitting a public key in an outgoing message to a recipient so that the recipient need not retrieve the sender's public key from the repository (Koehler, col. 2, ll. 23-25). This cited section teaches transmission of a public key, and not a certificate (role or otherwise). Accordingly, Koehler does not teach transmitting the role certificate to the role member, as recited in claims 22 and 53.

The Office Action dated November 10, 2004, did not address the element of selecting the expired role certificate from the list of roles by the role member for recovery, as recited in claims 22 and 53. The Office Action's deficiency in not addressing this claim element was argued in the response to the Office Action dated November 10, 2004. However, the Office Action dated May 3, 2005, maintains the rejection of claims 22 and 53 without having addressed this claim element. As discussed in the response to the Office Action dated November 10, 2004, Koehler does not teach selecting the expired role certificate from the list of roles by the role member for recovery, as recited in claims 22 and 53.

For all of the reasons described above, Koehler does not anticipate claims 22 and 53. Withdrawal of the rejection of claim 22, as well as claims 23-25 which depend therefrom, and claim 53, as well as claims 54-56 which depend therefrom, is respectfully requested.

Claims 26 and 57 recite a method of revoking a role certificate and an associated role by a role administrator comprising transmitting a request to revoke the role certificate of a role member, wherein the role member is a member of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members. As described above with regard to claims 11 and 42, Koehler does not teach the use of a role certificate, and thus claims 26 and 57 should be allowable.

In addition, claims 26 and 57 also recite transmitting a request to revoke the role certificate and the associated role by the role administrator for the role certificate along with a signature certificate for the role administrator, searching a database for all role certificates in which the role administrator is listed as a role administrator, and displaying to the role administrator all role certificates discovered. The response to the Office Action dated November

10, 2004, proffers a number of arguments in response to the rejection of claims 26 and 57 (Response to Office Action dated November 10, 2004, pages 26-27). None of these arguments were addressed in the Office Action dated May 3, 2005. Representative for Applicant therefore reiterates the previously stated arguments below and respectfully requests that the Examiner consider them.

The Office Action dated May 3, 2005 (page 7), asserts that Koehler discloses transmitting a request to revoke a role certificate and the associated role (citing Koehler, col. 6, ll. 56-62). The cited section describes that a verification server checks if a certificate authority's certificate is authentic and rejects a client's request for verification if it is not (Koehler, col. 6, ll. 56-62). Neither this cited section, nor any other section of Koehler, teaches transmitting a request to revoke the role certificate and the associated role by the role administrator for the role certificate along with a signature certificate for the role administrator, as recited in claims 26 and 57. The Office Action dated May 3, 2005 (page 7), further asserts that Koehler discloses searching a database for all role certificates in which the role administrator is listed as a role administrator (citing Koehler, col. 8, ll. 28-31). Koehler teaches that a certificate revocation list is searched for digital certificates of users depending on a timestamp (Koehler, col. 8, ll. 28-31), but does not teach searching a database for all role certificates in which the role administrator is listed as a role administrator, as recited in claims 26 and 57. The Office Action dated May 3, 2005 (page 7), further asserts that Koehler discloses displaying to the role administrator all role certificates revoked (citing Koehler, col. 3, ll. 25-30). It is respectfully submitted that the Office Action dated May 3, 2005, has mischaracterized the language of claims 26 and 57, in that claims 26 and 57 recite displaying to the role administrator all role certificates "discovered," and not "revoked." Koehler does not teach a list of displaying to the role administrator all role certificates discovered, as recited in claims 26 and 57. Accordingly, claims 26 and 57 are not anticipated by Koehler. Withdrawal of the rejection of claim 26, as well as claims 27 and 28 which depend therefrom, and claim 57, as well as claims 58 and 59 which depend therefrom, is respectfully requested.

Claim 63 recites a role certificate for organizational encryption and for use as an organizational stamp or seal comprising extensions having a plurality of bits which designate characteristics associated with the role certificate, wherein when a bit for encryption is set and a bit for signature is set, the role certificate may be used for both digital signatures and encryption, and a policy defining the limitations on valid usage of the role certificate. The response to the Office Action dated November 10, 2004, proffers an argument in response to the rejection of claim 63 (Response to Office Action dated November 10, 2004, pages 27-28). None of these arguments were addressed in the Office Action dated May 3, 2005. Representative for Applicant therefore reiterates the previously stated arguments below and respectfully requests that the Examiner consider them.

As described above regarding claim 11, Koehler does not teach the use of a role certificate. In addition, the Office Action dated May 3, 2005, asserts that Koehler teaches claim 63 at column 4, line 66 through column 5, line 5, and also at column 6, lines 5-8. The first cited section teaches that "a typical digital certificate [has] six data fields including owner information, the owner's public key, validity period, serial number, issuer information and issuer's digital signature." (Koehler, col. 4, line 66 through col. 5, line 2). The second cited section teaches that a verification cache is organized for efficient lookup of an item and is organized by owner and information type, with each cache entry storing information such as the item's timestamp, expiration data, issuer and user privileges (Koehler, col. 6, ll. 5-8). However, Koehler does not teach extensions having a plurality of bits which designate characteristics associated with the role certificate, wherein when a bit for encryption is set and a bit for signature is set, the role certificate may be used for both digital signatures and encryption, and a policy defining the limitations on valid usage of the role certificate, as recited in claim 63. Koehler, therefore, does not anticipate claim 63. Withdrawal of the rejection of claim 63, as well as claims 64-66 which depend therefrom, is respectfully requested.

Claim 66 recites that any time that the role certificate is used to sign on behalf of the organization, a signature certificate for the entity signing must be included. The response to the Office Action dated November 10, 2004, proffers an argument in response to the rejection of

claim 66 (Response to Office Action dated November 10, 2004, page 28). None of these arguments were addressed in the Office Action dated May 3, 2005. Representative for Applicant therefore reiterates the previously stated argument below and respectfully requests that the Examiner consider it.

Koehler teaches that a certificate authority digital signature is used to verify the authenticity of an issued certificate (Koehler, col. 5, ll. 17-20). However, Koehler does not teach that any time that the role certificate is used to sign on behalf of the organization, a signature certificate for the entity signing must be included, as recited in claim 66. Therefore, Koehler does not anticipate claim 66. Withdrawal of the rejection of claim 66 is respectfully requested.

For the reasons described above, claims 11-14, 16-22, 24-28, 42-45, 47-51-53, 55, 57-59, and 63-66 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

II. Rejection of Claims 1, 3-9, 32, and 34-40 Under 35 U.S.C. §103(a)

Claims 1, 3-9, 32, and 34-40 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,308,277 to Vaeth, et al. ("Vaeth") in view of U.S. Patent No. 5,659,616 to Sudia ("Sudia"). Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claims 1 and 32 recite a method and a computer program, respectively, of creating a role certificate comprising transmitting a role approval form, filled out and digitally signed by the user using a personal digital signature, wherein the user is a member of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members. The Office Action dated May 3, 2005, states that Vaeth does not disclose this claim element, but asserts that "Sudia discloses the use of group stamp and the use of role certificate for encryption information." (Office Action dated May 3, 2005, page 9, citing Sudia, col. 7, ll. 26-34). Representative for Applicant respectfully disagrees with this assertion. Sudia teaches that multiple signatures, or cosignatures, can be attached to a document, and that each signature on a document will contain an indication of the certificate

needed to validate the signature and a bit string containing the actual signature. (Sudia, col. 3, ll. 24-30). Therefore, a document's authenticity is determined by the multiple signatures within a document as verified with the validation certificate that is specified within the document itself. Sudia further teaches that:

Group and role certificates may be used in conjunction with a cosignature mechanism to simplify the construction of cosignature requirements. For example, a transaction might require the signatures of three occupants of the "purchasing agent" role. A user may also indicate the role in which he is acting by including the role in the signature computation as a (per-signer) signature attribute. The asserted role may be matched against a role certificate (or the user's attribute certificate) during verification. (Sudia, col. 7, ll. 26-34).

The above cited section indicates that the signatures on a given document must conform to a given role within the organization (exemplified as the "purchasing agent" role) to verify the document. The asserted role in which the multiple signees are acting is thus included in the document as one of the signature attributes. When the document is verified, it is compared to a role certificate to determine if the multiple signees satisfy the requisite role for verification. Therefore, Sudia does not teach or suggest a role certificate that acts as a group stamp and for encryption of information which may be decrypted by a plurality of group members, as recited in claims 1 and 32. Instead, the role certificate taught by Sudia is a verification certificate against which a given document is validated to determine if one or more signatures on the document are associated with a given role which is required for the verification. Accordingly, Sudia, individually or in combination with Vaeth or any other cited art, does not teach or suggest creating a role certificate comprising transmitting a role approval form, filled out and digitally signed by the user using a personal digital signature, wherein the user is a member of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members, as recited in claims 1 and 32. Withdrawal of the rejection of claims 1 and 32, as well as claims 2-6 and 33-37 which depend therefrom, respectively, is respectfully requested.

Claims 7 and 38 recite a method and computer program, respectively, of using a role certificate as an organizational stamp and for organizational encryption by a plurality of role members of a group comprising signing digitally the electronic form by the role member using the role certificate and signing digitally the electronic form by the role member using a personal signature certificate, wherein the role member is a member of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members. As described above with regard to claims 1 and 32, the combination of Vaeth and Sudia does not teach the use of a role certificate, and thus claims 7 and 38 should be allowable.

Additionally, the response to the Office Action dated November 10, 2004, proffers arguments in response to the rejection of claims 7 and 38 (Response to Office Action dated November 10, 2004, pages 19-20). These arguments were not addressed in the Office Action dated May 3, 2005. Representative for Applicant therefore reiterates the previously stated arguments below and respectfully requests that the Examiner consider them.

In rejecting claims 7 and 38, the Office Action dated May 3, 2005 (pages 10 and 11), cites the same section of the Vaeth (col. 4, ll. 34-54) that was cited for the rejection of claims 1 and 32. However, claims 1 and 7 (as well as claims 32 and 38) each claim methods for achieving different results, such that the Office Action dated May 3, 2005 (pages 10 and 11), is interpreting the teachings of Vaeth in two separate and conflicting ways. Further, claims 7 and 38 explicitly state that one individual (the role member) digitally signs the same electronic form using two different digital certificates. Vaeth teaches that a requester prepares a certificate request data submission and signs it with a private key (Vaeth, col. 4, ll. 34-37). However, Vaeth does not teach or suggest that the requester digitally signs the document with two separate certificates, and thus does not teach a role member signing digitally the electronic form by the role member using the role certificate and signing digitally the electronic form by the role member using a personal signature certificate, as recited in claims 7 and 38. As described above, the addition of Sudia does not cure the deficiencies of Vaeth to teach or suggest claims 7 and 38. Accordingly, the combination of Vaeth and Sudia does not teach or suggest claims 7 and 38.

Withdrawal of the rejection of claim 7, as well as claims 8-10 which depend therefrom, and claim 38, as well as claims 39-41 which depend therefrom, and is respectfully requested.

Claims 8 and 39 recite retrieving a policy associated with the role certificate by the entity. Claim 8 depends from claim 7, and claim 39 depends from claim 38, and thus both should be allowable for at least the reasons described above regarding claims 7 and 38. Additionally, the Office Action dated May 3, 2005, asserts that “Vaeth discusses retrieving of message.” (Office Action dated May 3, 2005, page 2). The Office Action provides no citation for this assertion. It is respectfully submitted that this assertion incorrectly characterizes the language of claims 8 and 39, in that claims 8 and 39 recite retrieving a *policy* associated with the role certificate by the entity (emphasis added), and not a message as asserted by the Office Action dated May 3, 2005. Both Vaeth and Sudia are silent as to policies associated with a digital certificate, and therefore do not teach or suggest retrieving a policy associated with the role certificate by the entity, as recited in claims 8 and 39. Withdrawal of the rejection of claims 8 and 39 is respectfully requested.

Claims 9 and 40 recite transmitting a public key portion of the role certificate by the role member to the entity, encrypting information by the entity, transmitting the information to any of the plurality of role members of the group, and decrypting the information by any of the plurality of role members of the group having the role certificate. Claim 9 depends from claim 7, and claim 40 depends from claim 38, and thus both should be allowable for at least the reasons described above regarding claims 7 and 38. Additionally, claims 9 and 40 recite that decrypting the information can be by any of the plurality of role members of the group having the role certificate. Vaeth teaches that a certified party can obtain a public key decrypting a message from a certifying authority using the certifying authority’s public key (Vaeth, col. 3, ll. 42-47). This cited section teaches that only a single party (the certified party) can decrypt the message from the certifying authority, but not that plural members of a group can decrypt the same message using the same certificate. Vaeth thus has no contemplation of a role certificate, and therefore, individually or in combination with Sudia, does not teach or suggest transmitting a public key portion of the role certificate by the role member to the entity, encrypting information

by the entity, transmitting the information to any of the plurality of role members of the group, and decrypting the information by any of the plurality of role members of the group having the role certificate, as recited in claims 9 and 40. Withdrawal of the rejection of claims 9 and 40 is respectfully requested.

For the reasons described above, claims 1, 3-9, 32, and 34-40 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

III. Rejection of Claims 2, 10, and 33 Under 35 U.S.C. §103(a)

Claims 2, 10, and 33 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Vaeth in view of U.S. Patent No. 6,275,859 to Wesley, et al. ("Wesley"). Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claims 2, 10, 33, and 41 recite that the role certificate comprises a public key, a private key, a signature algorithm ID, a validity period, extensions, and at least one policy. Wesley does not teach the use of a role certificate, such that the addition of Wesley does not cure the deficiencies of Vaeth to teach the recitations of claim 1 from which claim 2 depends, claim 7 from which claim 10 depends, claim 32 from which claim 33 depends, and claim 38 from which claim 41 depends. The Office Action dated May 3, 2005, also cites Wesley, at column 2, line 66 through column 3, line 5, to teach a role certificate, stating that the manner in which a node can participate in a multicast session (Office Action dated May 3, 2005, page 2). However, this teaching of Wesley does not contemplate a role certificate that acts as a group stamp and for encryption of information which may be decrypted by a plurality of group members, as recited in claims 1, 7, 32, and 38, from which claims 2, 10, 33, and 41 depend. Additionally, Wesley teaches that a participation certificate includes starting and ending times for the period authorized by a node and identifies the role of the node in the multicast session, such that it could be a repair node (col. 4, ll. 18-27). The Office Action dated May 3, 2005, cites this section in the Response to Arguments (page 2) to argue that this section teaches extensions and at least one policy, but provides no support for this argument. This cited section teaches nothing about extensions or at least one policy. Wesley does not teach or suggest that a certificate (role

certificate or otherwise) includes extensions and at least one policy, as recited in claims 2, 10, 33, and 41. Accordingly, the combination of Vaeth and Wesley does not teach or suggest claims 2, 10, 33, and 41. Withdrawal of the rejection of claim 2, as well as claims 3-6 which depend therefrom, claim 10, claim 33, as well as claims 34-37 which depends therefrom, and claim 41, is respectfully requested.

For the reasons described above, claims 2, 10, and 33 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

IV. Rejection of Claims 15 and 46 Under 35 U.S.C. §103(a)

Claims 15 and 46 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Koehler in view of Vaeth. Withdrawal of this rejection is respectfully requested for at least the following reasons.

The addition of Vaeth does not cure the deficiencies of Koehler to teach the recitations of claim 11 from which claim 15 depends, and claim 42 from which claim 46 depends. Additionally, the response to the Office Action dated November 10, 2004, proffers arguments in response to the rejection of claims 15 and 46 (Response to Office Action dated November 10, 2004, page 31). These arguments were not addressed in the Office Action dated May 3, 2005. Representative for Applicant therefore reiterates the previously stated arguments below and respectfully requests that the Examiner consider them.

Claims 15 and 46 recite that the private key portion of the role certificate is stored in a key recovery authority for recovery in case of loss or expiration. Vaeth teaches that a certificate request of a requester is stored at a certificate authority facility while the requester's certificate request is pending (Vaeth, col. 8, ll. 13-23). This section teaches that the requester does not yet have a certificate, and therefore does not yet have a private key that can be stored. Additionally, the certificate request storage is not for recovery in case of loss or expiration, as recited in claims 15 and 46, but is for awaiting approval or disapproval of the certificate request. Accordingly, the combination of Koehler and Vaeth does not teach or suggest claims 15 and 46. Withdrawal of the rejection of claims 15 and 46 is respectfully requested.

V. Rejection of Claims 23 and 54 Under 35 U.S.C. §103(a)

Claims 23 and 54 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Koehler in view of Wesley. Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claims 23 and 54 recite authenticating that the role member is either a member of the role or a role authority for the role prior to contacting the key recovery authority. The addition of Wesley does not cure the deficiencies of Koehler to teach the recitations of claims 22 and 53, from which claims 23 and 54 depend, respectively. In addition, the Office Action dated May 3, 2005, asserts that Wesley teaches authenticating that the role member is either a member of the role or a role authority for the role prior to contacting the key recovery authority by stating that “Wesley discloses verifying of role prior to the contacting repair nodes.” (Office Action dated May 3, 2005, page 13, citing Wesley, col. 3, ll. 6-20). The Office Action is therefore equating the key recovery authority recited in claims 23 and 54 with the repair nodes of Wesley. Wesley teaches that repair nodes are network nodes in a multi-cast network that provide reliability by caching all data sent by the sender and retransmits the cached data when requested by other participatory nodes (Wesley, col. 1, ll. 28-36). It is respectfully submitted that equating the key recovery authority recited in claims 23 and 54 with the repair nodes of Wesley is a severe mischaracterization of the key recovery authority. A key recovery authority is an entity in a PKI enterprise that stores copies of certificate keys and supplies them when needed due to the key being lost or expired (see, *e.g.*, Present Application, page 22, ll. 4-8, page 25, ll. 3-15, and Abstract, ll. 10-13). Therefore, the combination of Koehler and Wesley does not teach or suggest authenticating that the role member is either a member of the role or a role authority for the role prior to contacting the key recovery authority, as recited in claims 23 and 54. Withdrawal of the rejection of claims 23 and 54 is respectfully requested.

VI. Rejection of Claims 29, 30, 60, and 61 Under 35 U.S.C. §103(a)

Claims 29, 30, 60, and 61 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,487,658 to Micali ("Micali") in view of Sudia. Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claims 29 and 60 recite a method and computer program, respectively, of recovering a former role and an associated role certificate by a role administrator comprising searching a database to determine if any role members associated with the role certificate are still in the organization, wherein each of the role members are members of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members. The system of certificate revocation taught by Micali is for user digital certificates (see Micali, *e.g.*, col. 2, ll. 21-51), and nowhere describes a role certificate as described in the present application. Additionally, for the reasons described above regarding claim 1, Sudia fails to teach or suggest a role certificate that acts as a group stamp and for encryption of information which may be decrypted by a plurality of group members. Therefore, neither Micali nor Sudia, individually or in combination, contemplates the use of a role certificate, as recited in claims 29 and 60.

In addition, the response to the Office Action dated November 10, 2004, proffers arguments in response to the rejection of claims 29 and 60 (Response to Office Action dated November 10, 2004, pages 28-29). These arguments were not addressed in the Office Action dated May 3, 2005. Representative for Applicant therefore reiterates the previously stated arguments below and respectfully requests that the Examiner consider them.

Claims 29 and 60 further recite searching a database to determine if any role members associated with the role certificate are still in the organization, transmitting to at least one recovery agent a request for approval for the recovering of the role certificate when no role members are discovered to be in the organization, receiving approval from the at least one recovery agent for recovery of the role certificate, transmitting to the at least one recovery agent the role certificate retrieved when the recovery agent supplies an approval to recover the role certificate, and transmitting the role certificate to the role administrator by the recovery agent.

The Office Action dated May 3, 2005, asserts that claims 29 and 60 are taught by Micali (Office Action dated May 3, 2005, pages 13-14, citing Micali, col. 25, ll. 20-34, and col. 24, line 67 through col. 25, line 6). These cited section teach that a user can access a tamper-proof directory on secure hardware to determine if any certificates on a list have been revoked, the user receiving a digitally signed answer from the secure hardware (Micali, col. 25, ll. 20-34), and that a "shopkeeper" may wish to verify the validity of a received certificate in a transaction by consulting a directory (Micali, col. 24, line 67 through col. 25, line 6). It is respectfully submitted that neither this cited section, nor any other section of Micali, teaches the recovery of a digital certificate, and that Micali does not teach any of searching a database to determine if any role members associated with the role certificate are still in the organization, transmitting to at least one recovery agent a request for approval for the recovering of the role certificate when no role members are discovered to be in the organization, receiving approval from the at least one recovery agent for recovery of the role certificate, transmitting to the at least one recovery agent the role certificate retrieved when the recovery agent supplies an approval to recover the role certificate, and transmitting the role certificate to the role administrator by the recovery agent, as recited in claims 29 and 60. The addition of Sudia fails to cure the deficiencies of Micali to teach or suggest these elements of claims 29 and 60. Accordingly, neither Micali nor Sudia, alone or in combination, teaches or suggests claims 29 and 60. Withdrawal of the rejection of claim 29, as well as claims 30 and 31 which depend therefrom, and claim 60, as well as claims 61 and 62 which depend therefrom, is respectfully requested.

Claim 30 depends from claim 29 and claim 61 depends from claim 60, respectively. Claims 30 and 61 are thus allowable for at least the reasons described above with regard to claims 29 and 60. Additionally, the response to the Office Action dated November 10, 2004, proffers an argument in response to the rejection of claims 29 and 60 (Response to Office Action dated November 10, 2004, pages 28-29). This argument was not addressed in the Office Action dated May 3, 2005. Representative for Applicant therefore reiterates the previously stated argument below and respectfully requests that the Examiner consider it.

Claims 30 and 61 recite that the at least one recovery agent is at least two recovery agents and both recovery agents must approve recovery before recovery of the role certificate occurs. Micali teaches that a list of revoked certificates, digitally signed by a certificate authority, can be provided to a user in the form of a message digitally signed by secure hardware (Micali, col. 25, ll. 37-49). However, this cited section does not describe obtaining approval from two recovery agents to recover a certificate. The addition of Sudia does not cure the deficiencies of Micali to teach or suggest claims 30 and 61. Therefore, neither Micali nor Sudia, individually or in combination, teaches or suggests two recovery agents approving recovery before recovery of the role certificate occurs, as recited in claims 30 and 61. Withdrawal of the rejection of claims 30 and 61 is respectfully requested.

VII. Rejection of Claims 31 and 62 Under 35 U.S.C. §103(a)

Claims 31 and 62 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Micali in view of Sudia and further in view of Wesley. Withdrawal of this rejection is respectfully requested for at least the following reasons.

The addition of Wesley does not cure the deficiencies of Micali and Sudia to teach the recitations of claims 29 and 60, from which claims 31 and 62 depend, respectively. In addition, the response to the Office Action dated November 10, 2004, proffers arguments in response to the rejection of claims 29 and 60 (Response to Office Action dated November 10, 2004, page 33). These arguments were not addressed in the Office Action dated May 3, 2005. Representative for Applicant therefore reiterates the previously stated arguments below and respectfully requests that the Examiner consider them.

Claims 31 and 62 recite that both recovery agents must be authenticated as having authority to authorize the recovery of the role certificate prior to the role certificate being sent to the recovery agent. Wesley teaches that a certificate authority verifies a certificate's authenticity with the certificate's public key before issuing a participation certificate (Wesley, col. 4, ll. 3-6 and 15-17). The authentication taught by Wesley is to determine if a certificate is valid, and not to determine if recovery agents must be authenticated as having authority to authorize the

recovery of a role certificate, as recited in claims 31 and 62. Also, Wesley teaches that the authentication is prior to issuing a participation certificate, and not prior to the role certificate being sent to the recovery agent, as also recited in claims 31 and 62. Therefore, the combination of Micali, Wesley, and Sudia does not teach or suggest claims 31 and 62. Withdrawal of the rejection of claims 31 and 62 is respectfully requested.


CONCLUSION

In view of the foregoing remarks, Applicant respectfully submits that the present application is in condition for allowance. Applicant respectfully requests reconsideration of this application and that the application be passed to issue.

Please charge any deficiency or credit any overpayment in the fees for this amendment to our Deposit Account No. 20-0090.

Respectfully submitted,

Date 6/21/05


Christopher P. Harris
Registration No. 43,660

CUSTOMER NO.: 26,294

TAROLLI, SUNDHEIM, COVELL, & TUMMINO L.L.P.
526 SUPERIOR AVENUE, SUITE 1111
CLEVELAND, OHIO 44114-1400
Phone: (216) 621-2234
Fax: (216) 621-4072